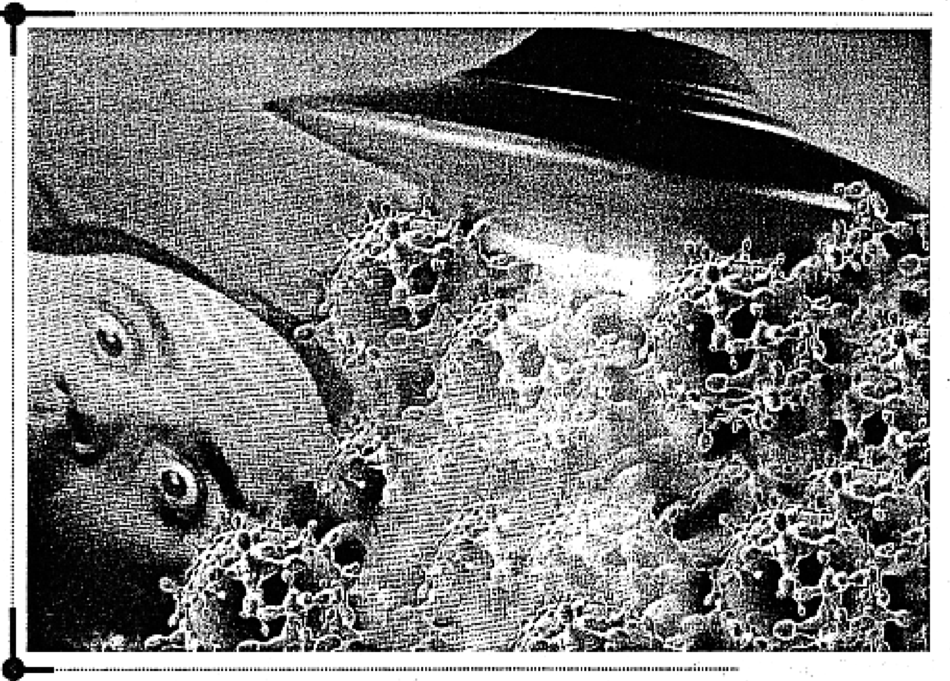


Schutz vor automatisierten Angriffen

Begegnungen der dritten Art

Die Nutzung von Netzwerken kann zu unerwünschten Begegnungen führen – mit Viren, Würmern und anderen Schädlingen. Und die gehen jetzt in die dritte Generation. IT-Verantwortliche sollten sich rechtzeitig auf die kommenden Begegnungen der dritten Art einstellen, um das Schlimmste zu verhindern.



Noch nie war es so einfach wie heute, IT-Systeme zu missbrauchen. Das Internet bietet Eindringlingen eine weltweite Angriffsfläche. Einbruchsversuche werden dadurch begünstigt, dass die Netzwerkgrenzen – auf Grund zahlreicher neuer Zugangspunkte wie Funknetze oder Virtual-Private-Networks – immer durchlässiger werden. Außerdem sind Netzwerke und Anwendungen heute komplexer, wodurch Tausende angreifbarer Schwachstellen entstehen. Und die Angriffe sind raffinierter: Neue, automatisierte Angriffswerkzeuge lassen sich leicht anwenden und überfluten das Internet im Handumdrehen mit zerstörerischen Bedrohungen, bevor die Sicherheitsadministratoren reagieren können.

Das Ziel besteht darin, in der ersten Stunde in so viele Systeme wie möglich einzubrechen, und so den Gegenschlag auszuschließen.

Die bei Sicherheitsattacken angewandten Methoden und Technologien haben sich drastisch verändert. Früher waren die Bedrohungen einfach strukturiert, lowtech und von begrenzter Reichweite. Heute werden die Angriffe immer raffinierter, teilweise deswegen, weil automatisierte Tools ihre Durchführung erleichtern. Man muss kein »Hackergenie« mehr sein, um weltweit immense Schäden anrichten zu können.

Raffinesse der Angriffe und Kenntnisse der Hacker

Zusätzlich begünstigt werden neue Einbrüche durch das Zusammenwirken weiterer technischer und betrieblicher Faktoren. Viele populäre, auf Standards basierende Netzwerkdienste wie Telnet, ftp und SNMP sind von Natur aus unsicher. Die Voreinstellungen von Systemen sind wohl bekannt und werden nach der Installation oft nicht verändert – hierzu gehören auch Login-Namen und Passwörter. Weil die verwendeten Technologien so komplex sind, kommt es oft zu Designfehlern, etwa, was das Setup und die Zugangskontrolle anbelangt. Tagtäglich werden Fehler bei der Software-Implementierung entdeckt und bekannt gemacht, beispielsweise mangelnde Eingabevalidierung oder Pufferüberläufe. Und schließlich lösen die Nutzer oft selbst unwissentlich Einbrüche aus – durch scheinbar harmlose E-Mails oder einfach dadurch, dass sie im Internet surfen.

All diese Faktoren tragen zu der rasant steigenden Zahl neuer Sicherheitsereignisse bei, die dem CERT-Coordination-Center gemeldet werden. In der Zeit von 1998 bis einschließlich 2002 stieg die Zahl der Vorkommnisse um 2099 Prozent – das ist eine durchschnittliche jährliche Gesamtsteigerungsrate von 116 Prozent (siehe www.cert.org/stats/cert_stats.html). Die Bedrohungen, die die erwähnten Sicherheitsprobleme ausnutzen, treten nunmehr in die dritte Generation ein. Der nachfolgende Überblick zeigt, wie sich die Art der Bedrohungen verändert hat.

Bedrohungen der ersten Generation: Bei diesen Bedrohungen handelt es sich um Angriffe vom Virentyp, die sich über E-Mail und gemeinsame Dateinutzung verbreiteten. Zu ihren wesentlichen Merkmalen gehört, dass menschliches Zutun erforderlich ist, damit sie sich reproduzieren und verbreiten können – zum Beispiel, dass ein Nutzer einen infizierten Dateianhang öffnet. Beispiele für diesen Typ sind der Makro-Virus Melissa, der VB-Script-Wurm Loveletter und in jüngster Zeit der Fizzer-Virus. Es existieren wirkungsvolle Technologien, um diese Bedrohungen zu erkennen und zu beseitigen; Hersteller von Antiviren-Produkten stehen an vorderster Front, wenn es darum geht, diese Gefahren zu identifizieren und die Kunden vor ihnen zu schützen. Antiviren-Produkte werden kontinuierlich aktualisiert, damit sie in der Lage sind, neu aufgekommene Bedrohungen von diesem Typ zu erkennen.

Bedrohungen der zweiten Generation: In dieser Kategorie herrschen aktive Würmer vor, die Systeme und Anwendungen angreifen. Sie dringen ein, indem sie Sicherheitslücken in den Systemen und Applikationen ausnutzen; Anwenderaktionen sind dazu nicht erforderlich. Sie replizieren sich automatisch; ebenso werden neue Opfer automatisch identifiziert und ins Visier genommen. Die Verbreitungsstrategie kann unterschiedlich sein, doch häufig wird eine Zufallsfunktion mit nicht-destruktiven Nutzlasten eingesetzt. Oft handelt es sich um »Blended Threats« – kombinierte Angriffe, die Viren, Trojaner und die automatische Ausnutzung bekannter Sicherheitslücken umfassen. Beispiele aus der jüngsten Zeit sind der Wurm Spida

(SQLsnake) (5/02), der Wurm Bugbear (9/02), der Wurm Slapper (9/02) und der SQL-Slammer-Wurm (1/03). Schwachstellenanalysen sind eine effektive Methode, um Sicherheitslücken proaktiv zu ermitteln und zu beheben, bevor sie von solcher Malware ausgenutzt werden können.

Bedrohungen der dritten Generation: Die Bedrohungen der dritten Generation unterscheiden sich von den früheren sowohl durch die Fortpflanzungsgeschwindigkeit als auch durch die Strategien, mit denen sie ihre Opfer auswählen. Das Ziel besteht darin, in der ersten Stunde in so viele Systeme wie nur möglich einzubrechen, weil dadurch ein Gegenschlag praktisch ausgeschlossen wird. Die Bedrohungen dieser Generation werden neue anfällige Ziele systematisch im Voraus identifizieren, um die Schäden zu maximieren. Teilweise werden sie unbekannte Sicherheitslücken ausnutzen und mehrere Angriffsvektoren führen, was die Abwehr erschwert. Es ist unbedingt erforderlich, regelmäßige Sicherheitsaudits durchzuführen, damit Schwachstellen gefunden und behoben werden können, bevor Bedrohungen der dritten Generation gestartet werden.

Anatomie künftiger Sicherheitsbedrohungen

Jüngste Sicherheitsattacken weisen erste Merkmale von Malware der dritten Generation auf – und demonstrieren eindringlich, welch verheerende Auswirkungen künftige Angriffe haben können. So befiel beispielsweise der SQL-Slammer-Wurm am 25. Januar 2003 innerhalb kürzester Zeit mehr als 120000 Server, auf denen Microsoft-SQL-Server läuft, legte dadurch den Internet-Verkehr in Südkorea lahm, setzte die Kassenautomaten einer US-Großbank außer Gefecht, unterbrach den Betrieb von 911 Call-Centern in Seattle und verursachte weltweit weitere schwere Störungen. SQL-Slammer war der schnellste Wurm, den es je gab – mehr als 90 Prozent der betroffenen Hosts wurden innerhalb von 10 Minuten infiziert. In der ersten Minute verdoppelte sich die Größe der infizierten Population alle 8,5 Sekunden; nach nur drei Minuten war eine Gesamt-Scanning-Rate von mehr als 55 Millionen Scans pro Sekunde erreicht. SQL-Slammer zeigt bereits jene ultraschnelle Fortpflanzung, die für Angriffe der dritten Generation charakteristisch ist, gilt aber immer noch als Bedrohung der zweiten Generation. Der Exploit nutzte eine wohl bekannte, dokumentierte Sicherheitslücke aus und beschränkte sich auf einen Angriffsvektor. Sämtliche Host-Einbrüche hätten sich durch Anwendung eines Patches verhindern lassen, den Microsoft sechs Monate vor dem Angriff bekannt gegeben hatte.

Drei Eigenschaften der dritten Generation

Ultraschnelle Verbreitung: Schnellere Fortpflanzung ist aus Hacker-Sicht wünschenswert – sie verhindert ein rechtzeitiges Eingreifen der Sicherheitsadministratoren und richtet deshalb größere Schäden an. Die Autoren von SQL-Slammer setzten eine Strategie ein, bei der zufällige Adressen gescannt wurden, um neue Ziele aufzuspüren, und erzielten damit exponentielles Wachstum. Diese Strategie erbrachte schnell gute Resultate, weil UDP als verbindungsloses Übertragungsprotokoll verwendet wurde. Andererseits jedoch überlastete SQL-Slammer rasch die von SQL-Server-Hosts verwendeten Netzwerke und behinderte sich damit selbst. Angriffe der dritten Generation werden noch bessere Durchdringung erzielen, indem ihre Autoren Systeme mit anvisierten Schwachstellen vorkompilieren – und erst dann losschlagen. Mittels Vorkompilation können Angreifer das Internet scannen, die Erfolgschancen für einen Angriff einschätzen und viel versprechende Ziele katalogisieren. Vorkompilation ist eine besonders effiziente Strategie: Der Angreifer verwendet sozusagen eine Landkarte, um geplante Ziele schnell zu er-

> **Info**
>
> **Entwicklung der Bedrohungen**
>
> 1. Generation: Viren verbreiten sich durch Anwenderaktionen wie E-Mail und gemeinsame Dateinutzung.
> 2. Generation: Aktive Würmer nutzen bekannte Schwachstellen aus. Sie verbreiten sich automatisch und ohne Anwendereinwirkung.
> 3. Generation (die Zukunft): Ultraschnelle Fortpflanzung, unbekannte Schwachstellen, mehrere Angriffsvektoren.

reichen, anstatt wahllos alle auf dem Weg liegenden Straßen abzufahren. Mit Vorkompilation lassen sich blitzartige, immer schneller werdende Angriffe durchführen – ähnlich einer Lawine, die während ihrer kurzen Lebensdauer verheerende Schäden anrichten kann.

Ausnutzung bekannter und unbekannter Sicherheitslücken: Bei praktisch allen Angriffen in der Vergangenheit wurden bekannte Sicherheitslücken ausgenutzt. Ein wesentlicher Grund hierfür liegt darin, dass die Entdeckung neuer Schwachstellen harte Arbeit ist und die technischen Fähigkeiten des durchschnittlichen Angreifers übersteigt. So stammt beispielsweise der Exploit-Code für die Kernkomponente von SQL-Slammer aus Forschungsergebnissen, die 2002 auf einer Black-Hat-Sicherheitskonferenz vorgestellt wurden. Auch künftige Angreifer werden sich gerne die Früchte schnappen, die sie durch Ausnutzung bekannter Sicherheitslücken leicht ernten können. Sie werden aber auch Schwachstellen ausnutzen, die nicht bekannt sind und vor denen die Sicherheitsadministratoren nicht gewarnt wurden. Durch vorkompilierte Angriffe wird das Gesamtuniversum angreifbarer Ziele wachsen. In der Vergangenheit richteten sich die Bedrohungen hauptsächlich gegen die populärsten Applikationen und Systeme, weil hier mit Techniken der zufälligen Fortpflanzung die größte Stoßkraft zu erzielen war. In Zukunft werden selbst ungebräuchliche Anwendungen und Geräte gefährdet sein; automatisierte, vorkompilierte Angriffe werden auch deren spezielle Schwachstellen aufspüren und ausnutzen können. Das Risiko von Angriffen auf unbekannte Schwachstellen steigt, je mehr es in diversen internationalen Auseinandersetzungen technisch gewiefte und mit umfangreichen Ressourcen ausgestattete Parteien gibt, die es darauf anlegen, bei ihren jeweiligen Feinden digitale Verwüstungen anzurichten.

Mehrere Angriffsvektoren: Sicherheitsbedrohungen der dritten Generation werden mehrere Angriffsvektoren führen. Besonders anfällig werden viele neue Technologien sein, weil sie mit keinen weit reichenden Funktionen zur Erkennung von Bedrohungen und zum Schutz vor ihnen ausgestattet sind. Zu diesen Technologien gehören: Instant-Messaging (IM), Funknetz-Infrastruktur sowie Voice-over-IP-basierte Systeme.

Server, die als Knotenpunkte für Instant-Messaging fungieren, werden zu beliebten Angriffszielen werden. IM-Kommunikation ist für gewöhnlich unverschlüsselt und verfügt nur über begrenzte Technologien zum Gateway-Schutz. Außerdem beschränkt sich die Erkennung von Bedrohungen bei IM weitgehend auf die Desktop-Anwendungen. Die umfangreichen File-Sharing-Möglichkeiten werden zum großen Problem werden – so können etwa IM-Anwendungen zum Transport von Daten und Dateien missbraucht werden, die Angriffscode enthalten. Außerdem werden die Bedrohungen der dritten Generation polymorphe Verschleierungs- und Verschlüsselungstechniken einsetzen, um während eines Angriffs nicht entdeckt zu werden.

Automatisierung als Waffe gegen die Bedrohungen

Angesichts der Folgen, die die schnelle Ausbreitung haben wird, müssen die Sicherheitsadministratoren auf neue Weise mit den Gefahren umgehen, die ihre Netzwerke bedrohen. In der Vergangenheit betrug die Lebenszykluskurve von der Entdeckung einer Schwachstelle bis zu ihrer großflächigen Ausnutzung ein oder zwei Jahre. Doch jetzt werden Gegenmaßnahmen immer dringlicher, weil sich die Kurve zwischen Entdeckung und Angriff zunehmend verengt – SQL-Slammer schlug sechs Monate nach der Entdeckung der Schwachstelle zu, Nimda vier Monate und Slapper nur sechs Wochen, nachdem die entsprechende Sicherheitslücke entdeckt worden war.

Die Bedrohungen der Zukunft machen es erforderlich, mit gleichen Mitteln zurückzuschlagen, denn die Angreifer nützen alle Vorteile automatisierter Tools. Mit Hilfe dieser tückischen Technologie können sie automatisch nach potenziellen Opfern scannen, anfällige Systeme kompromittieren, Angriffscode programmieren, der sich nach dem Eindringen selbstständig reproduziert, und das Management und die Kontrolle des Angriffscodes zum Zweck künftiger Aktivitäten zentralisieren. Automatisierte Angriffe bekämpft man am effektivsten dadurch, dass man die Abwehrmaßnahmen automatisiert. Einige Abwehrstrategien sind folgende.

Regelmäßige Audits der Sicherheitssysteme, bei denen Schwachstellen in Systemen und Anwendungen analysiert werden, sind ein wichtiges Mittel, um eine starke Abwehr zu gewährleisten. Die Methoden reichen von herkömmlichen Durchdringungstests bis hin zu neuen, automatisierten Diensten, die über das Web durchgeführt werden. Häufige Audits stellen sicher, dass die Administratoren schnell und effektiv auf neu entstandene Angriffspunkte reagieren können. Die Schlüsselelemente eines gründlichen Audits sind:

- Identifizierung der Netztopologie und sämtlicher Zugangspunkte – von außerhalb und innerhalb der Unternehmens-Firewall,
- Identifizierung aller Dienste, Betriebssysteme und Anwendungen auf allen ans Netzwerk angebundenen IPs, um festzustellen, welche Sicherheitslücken eventuell bestehen könnten,
- Identifizierung und Priorisierung kritischer Sicherheitslücken im Unternehmen sowie
- Auswahl geeigneter Abhilfemaßnahmen für die gefundenen Sicherheitslücken, wie Patches und neue Konfigurationseinstellungen.

Der Einsatz von Antiviren-Software ist unerlässlich, um bekannte Bedrohungen zu blockieren, besonders, wenn diese nach einer ersten Angriffswelle periodisch wiederkehren. Herkömmliche Antiviren-Software vergleicht die Anwendungsdateien mit einer Datei, die Viren-»Signaturen« enthält. Zu einer effektiven Abwehr gehört, dass die Nutzer jeweils die neueste Version der vom Hersteller gelieferten Signaturdatei installieren.

Anbieter von Anwendungsprogrammen geben häufig Patches heraus, die die bestehende Anwendung modifizieren, um Sicherheitslücken zu schließen, ohne den gesamten Code zu ersetzen. Der rechtzeitige Einsatz von Patches ist eine der effektivsten Abwehrmaßnahmen überhaupt. Um auf neue Patches aufmerksam zu werden, können die IT-Verantwortlichen auf die Ankündigungen der Anbieter achten und auf Meldungen reagieren, die bei Sicherheitsaudits ausgegeben werden. Durch rechtzeitigen Einsatz von Security-Patches kann ein Unternehmen die meisten Angriffe verhindern.

Und schließlich: Sicherheit ist ein bewegliches Ziel, und deshalb sollten Unternehmen ihre internen Sicherheitsrichtlinien und die Maßnahmen zu deren Durchsetzung regelmäßig überprüfen. Hierzu können sie die Trendanalysen nützen, die im Rahmen von regelmäßigen Sicherheitsaudits generiert werden: Mit Hilfe dieser Daten lässt sich gewährleisten, dass die Sicherheitssysteme wirklich dazu beitragen, den sich ständig wandelnden Bedrohungen wirksam entgegenzutreten.

Fazit

Die Angriffe auf die Netzwerksicherheit werden immer zahlreicher und raffinierter. Hacker nützen die Erfahrungen, um eine neue Generation automatisierter Bedrohungen zu entwickeln. Die Angriffe der Zukunft werden sich schneller fortpflanzen, als jede menschenmögliche Gegenwehr greifen kann. Die rechtzeitige und umfassende Erkennung von Sicherheitslücken und die rasche Durchführung von Abhilfemaßnahmen sind die wirkungsvollsten Vorkehrungen, die die Sicherheitsadministratoren treffen können, um automatisierte Angriffe abzuwehren und die Sicherheit ihrer Netzwerke zu wahren.

Dr. Gerhard Eschelbeck, Chief Technologie Officer und Vice President of Engineering Qualys